What is claimed is:

1. A method of generating a pseudo-random number, said method comprising the steps of:

(a) Establish initialization values for output series of pseudo-random number matrices $X_1 - X_k$;

(b) Establish initialization values for variable transition matrices $A_{1,1} - A_{k,1}$;

(c) Establish initialization values for variable offset matrices $B_{1,1} - B_{j,1}$;

(d) Establish first modulus operators $m_{1,1} - m_{i,1}$;

(e) Apply said transition matrices $A_{1,1} - A_{k,1}$ to said output series of pseudo-random number matrices $X_1 - X_k$ to generate a first intermediate matrix value $X_{firsttemp}$;

(f) Apply said offset matrices $B_{1,1} - B_{j,1}$ to said first intermediate matrix value $X_{firsttemp}$ to generate a second intermediate matrix value X_{temp}; and

(g) Sequentially apply said first modulus operators $m_{1,1} - m_{i,1}$ to said second intermediate matrix value X_{temp} to generate an output value of pseudo-random number matrix X_n from which at least one pseudo-random number is extracted.

2. A method of generating a plurality of pseudo-random numbers, said method comprising the steps of:

(a) Establish initialization values for output series of pseudo-random number matrices $X_1 - X_k$;

(b) Establish initialization values for variable transition matrices $A_{1,1} - A_{k,1}$;

(c) Establish initialization values for variable offset matrices $B_{1,1} - B_{j,1}$;

(d) Establish first modulus operators $m_{1,1} - m_{i,1}$;

(e) Apply said transition matrices $A_{1,1} - A_{k,1}$ to said output series of pseudo-random number matrices $X_1 - X_k$ to generate a first intermediate matrix value $X_{firsttemp}$;

(f) Apply said offset matrices $B_{1,1} - B_{j,1}$ to said first intermediate matrix value $X_{firsttemp}$ to generate a second intermediate matrix value X_{temp};

(g) Sequentially apply said first modulus operators $m_{1,1} - m_{i,1}$ to said second intermediate matrix value X_{temp} to generate a first output value of pseudo-random number matrix X_n from which at least one pseudo-random number is extracted;

(h) Store said first output value matrix X_n in a storage register to establish an updated output series of pseudo-random number matrices;

(i) Update said transition matrices $A_{1,1} - A_{k,1}$ through updating process to create updated transition matrices $A_{1,2} - A_{k,2}$;

(j) Apply said updated transition matrices $A_{1,2} - A_{k,2}$ to said updated output series of pseudo-random number matrices $X_{n-k+1} - X_n$ to generate an updated first intermediate matrix value $X_{firsttemp}$;

(k) Update said offset matrices $B_{1,1} - B_{j,1}$ through updating process to create updated offset matrices $B_{1,2} - B_{j,2}$;

(l) Apply said updated offset matrices $B_{1,2} - B_{j,2}$ to said updated first intermediate matrix value $X_{firsttemp}$ to generate an updated second intermediate matrix value X_{temp};

(m) Update said first modulus operators $m_{1,1} - m_{i,1}$ through updating process to create updated first modulus operators $m_{1,2} - m_{i,2}$;

(n) Sequentially apply said updated first modulus operators $m_{1,2} - m_{i,2}$ to said updated second intermediate matrix value X_{temp} to generate a second output value of pseudo-random number matrix X_{n+1} from which at least one pseudo-random number is extracted; and

(o) Store said second pseudo-random number matrix X_{n+1} in said storage register of pseudo-random number matrices.

3. A method of generating a plurality of pseudo-random numbers according to claim 2, wherein said steps i. through o. are repeated to generate a desired number d of pseudo-random number matrices X_{n+d} from which a plurality of pseudo-random numbers are extracted.

4. A method according to claim 2 further comprising the step of:

Selecting a first subset of said pseudo-random numbers from said updated output series of pseudo-random number matrices .

5. A method according to claim 1, claim 2, or claim 3, wherein k = 1 so that a single variable transition matrix is used.

6. A method according to claim 1, claim 2, or claim 3, where j = 1 so that a single variable offset matrix is used.

7. A method according to claim 1, claim 2, or claim 3, where i = 1 so that a single modulus operator is used.

8. A method according to claim 2, further comprising the steps of:

(a) Establish second modulus operators $r_{1,1} - r_{g,1}$;

(b) Sequentially apply and update second modulus operators $r_{1,1} - r_{g,1}$, $r_{1,2} - r_{g,2}$, ... $r_{1,n+d-k} - r_{g,n+d-k}$ to said updated output series of pseudo-random number matrices to generate a second output series of pseudo-random number matrices.

9. A method according to claim 8, further comprising the step of:

Selecting a second subset of said pseudo-random numbers from said second output series of pseudo-random number matrices.

10. A method according to claim 1, claim 2, or claim 3:

(a) Wherein said first modulus operators $m_{1,1} - m_{j,1}$, $m_{1,2} - m_{j,2}$, ... $m_{1,n+d-k} - m_{j,n+d-k}$ comprise a uniform variable modular reduction, and

(b) Further comprising the step of discarding certain pseudo-random numbers which are not uniformly distributed.

11. A method according to claim 8:

(a) Wherein said second modulus operators $r_{1,1} - r_{g,1}$, $r_{1,2} - r_{g,2}$, ... $r_{1,n+d-k} - r_{g,n+d-k}$ comprise a uniform variable modular reduction, and

(b) Further comprising the step of discarding certain pseudo-random numbers which are not uniformly distributed.

12. A method according to claim 2 or claim 3, further comprising the steps of:

(a) Create at least one other storage register of pseudo-random number matrices by separately taking steps a – o;

(b) Create temporary composite pseudo-random number matrices by combining each resulting storage register of pseudo-random number matrices through at least one mathematical operation;

(c) Create final composite pseudo-random number matrices by applying variable modular reduction to said temporary composite pseudo-random number matrices; and

(d) Select a subset of pseudo-random numbers from said resulting final composite pseudo-random number matrices

13. A method according to claim 1, claim 2, or claim 3 further comprising:

(a) Apply an invertibility evaluation module to each second intermediate matrix value $X_{temp;}$

(b) Adjust offset matrices $B_{1,1} - B_{j,1}$, $B_{1,2} - B_{j,2}$, ... $B_{1,n+d-1} - B_{j,n+d-1}$, so that said second intermediate matrix value X_{temp} is non-invertible;

(c) Sequentially apply said first modulus operators $m_{1,1} - m_{i,1}$ to said non-invertible second intermediate matrix value X_{temp} to generate output value of non-invertible pseudo-random number matrix X_n from which at least one pseudo-random number is extracted; and

(d) Select a subset of pseudo-random number output values from said non-invertible pseudo-random number matrices

14. An apparatus for generating a pseudo-random number, said apparatus comprising:

(a) Output matrices initialization means for establishing initialization values for output series of pseudo-random number matrices $X_1 - X_k$;

(b) Transition matrices initialization means for establishing initialization values for variable transition matrices $A_{1,1} - A_{k,1}$;

(c) Offset matrices initialization means for establishing initialization values for variable offset matrices $B_{1,1} - B_{j,1}$;

(d) Modulus operator means for establishing first modulus operators $m_{1,1} - m_{i,1}$;

(e) First application means for applying said transition matrices $A_{1,1} - A_{k,1}$ to said output series of pseudo-random number matrices $X_1 - X_k$ to generate a first intermediate matrix value $X_{firsttemp}$;

(f) Second application means for applying said offset matrices $B_{1,1} - B_{j,1}$ to said first intermediate matrix value $X_{firsttemp}$ to generate a second intermediate matrix value X_{temp}; and

(g) Third application means for sequentially applying said first modulus operators $m_{1,1} - m_{i,1}$ to said second intermediate matrix value X_{temp} to generate an output value of pseudo-random number matrix X_n from which at least one pseudo-random number is extracted.

15. An apparatus for generating a plurality of pseudo-random numbers, said apparatus comprising:

(a) Output matrices initialization means for establishing initialization values for output series of pseudo-random number matrices $X_1 - X_k$;

(b) Transition matrices initialization means for establishing initialization values for variable transition matrices $A_{1,1} - A_{k,1}$;

(c) Offset matrices initialization means for establishing initialization values for variable offset matrices $B_{1,1} - B_{j,1}$;

(d) Modulus operator means for establishing first modulus operators $m_{1,1} - m_{i,1}$;

(f) First application means for applying said transition matrices $A_{1,1} - A_{k,1}$ to said output series of pseudo-random number matrices $X_1 - X_k$ to generate a first intermediate matrix value $X_{firsttemp}$;

(g) Second application means for applying said offset matrices $B_{1,1} - B_{j,1}$ to said first intermediate matrix value $X_{firsttemp}$ to generate a second intermediate matrix value X_{temp};

(h) Third application means for sequentially applying said first modulus operators $m_{1,1} - m_{i,1}$ to said second intermediate matrix value X_{temp} to generate a first output value of pseudo-random number matrix X_n from which at least one pseudo-random number is extracted;

(i) Storage means for storing said first output value matrix X_n in a storage register to establish an updated output series of pseudo-random number matrices;

(j) Transition matrices updating means for updating said transition matrices $A_{1,1} - A_{k,1}$ to create updated transition matrices $A_{1,2} - A_{k,2}$;

(k) Fourth application means for applying said updated transition matrices $A_{1,2} - A_{k,2}$ to said updated output series of pseudo-random number matrices $X_{n-k+1} - X_n$ to generate an updated first intermediate matrix value $X_{firsttemp}$;

(l) Offset matrices updating means for updating said offset matrices $B_{1,1} - B_{j,1}$ to create updated offset matrices $B_{1,2} - B_{j,2}$;

(m) Fifth application means for applying said updated offset matrices $B_{1,2} - B_{j,2}$ to said updated first intermediate matrix value $X_{firsttemp}$ to generate an updated second intermediate matrix value X_{temp};

(n) Modulus operator updating means for updating said first modulus operators $m_{1,1} - m_{i,1}$ to create updated first modulus operators $m_{1,2} - m_{i,2}$;

(o) Sixth application means for sequentially applying said updated first modulus operators $m_{1,2} - m_{i,2}$ to said updated second intermediate matrix value X_{temp} to generate a second output value of pseudo-random number matrix X_{n+1} from which at least one pseudo-random number is extracted; and

(p) Second storage means for storing said second pseudo-random number matrix X_{n+1} in said storage register of pseudo-random number matrices.